The Ethics in Cloud Computing

Oktay Tontaş
Polytechnic of Coimbra
ISEC – Coimbra Institute of Engineering
3030-199 Coimbra, Portugal
oktay1125@gmail.com

Jorge Bernardino
Polytechnic of Coimbra
ISEC – Coimbra Institute of Engineering
3030-199 Coimbra, Portugal
jorge@isec.pt

***Abstract*—Several issues of ethics can arise in the development of cloud computing. Cloud computing may seem like a rather unclear term, so we can have a look at the issue and its impact. Cloud computing is basically computer storage like a service that users can use cloud computing to store their files and retrieve them whenever they want, or use the cloud computing's power to edit or collaborate on files, without having to know any technical knowledge of how cloud computing works. The purpose of this paper is to identify ethical issues that result from the essential nature of cloud computing. It is also describes how these features are identified, and it concludes by discussing means of addressing them.**

Keywords—Ethic; Cloud Computing; Hacker Ethic; Cyber Security; IaaS; PaaS; SaaS.

I. INTRODUCTION

The National Institute of Standards and Technology defines cloud computing in the following way: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [1]. Cloud computing has some problems and issues to be solved and it can lead to numerous ethical issues. One of them is privacy. When users store their personal data in clouds, they do not want third parties to reach them. Similar issues can occur like confidentiality.

Cloud computing warrants ethical analysis but the question is how to do this ethical analysis. Are there common ethical issues in cloud computing? How will we know which issues count as ethical? How are they to be evaluated? This paper aims to find some answers to these questions.

Cloud computing is based on a paradigm shift with deep implications for computing ethics. The main elements of this shift are:

- The control is left to third-party services;
- The data is stored on multiple sites administered by several organizations; and
- Multiple services interoperate across the network.

Unauthorized access, data corruption, infrastructure failure, and service unavailability are some of the risks related to relinquishing the control to third-party services; moreover, whenever a problem occurs, it is difficult to identify the source and the entity causing it. Systems can span the boundaries of multiple organizations and cross security borders, a process called deperimeterization [2].

The complex structure of cloud services can make it difficult to determine who is responsible in case something undesirable happens. In a complex chain of events or systems, many entities contribute to an action, with undesirable consequences. Some of them have the opportunity to prevent these consequences, and therefore no one can be held responsible – the so-called "problem of many hands".

Cloud service providers have already collected petabytes of sensitive personal information stored in data centers around the world. The acceptance of cloud computing therefore will be determined by privacy issues addressed by these companies and the countries where the data centers are located. Privacy is affected by cultural differences; though some cultures favor privacy, other cultures emphasize community, and this leads to an undecided opinion toward privacy on the Internet, which is a global system.

The question of what can be done proactively about ethics of cloud computing does not have easy answers; many undesirable phenomena in cloud computing will only appear in time. However, the need for rules and regulations for the governance of cloud computing is obvious. The term governance means the manner in which something is governed or regulated, the method of management, or the system of regulations. Clear attention to ethics must be paid by governmental organizations providing research funding for cloud computing; private companies are less restricted by ethics oversight and governance arrangements are more creative to profit generation [3].

This paper is structured as follows. In Section II, we review and define the concept of cloud computing, pointing their essential characteristics, service models, and deployment models. In Section III, we give a brief overview of cloud computing history and its evolution. In Section IV, we present the service models associated to cloud computing stack. Section V shows same examples of cloud computing services. In Section VI we describe how cloud computing can evolve in the future and Section VII points its main benefits. In Section VIII we describe the hacker ethic and cyber security is discussed in Section IX. Finally, in Section X, concluding remarks are presented.

978-1-5090-3912-8/16/$31.00 ©2016 IEEE

II. CLOUD COMPUTING

According to COSO, "Cloud computing is a computing resource deployment and supply model that enables an organization to obtain its computing resources and applications from any location via an Internet connection" [4].

Depending on the cloud solution model an organization adopts, all or parts of the organization's hardware, software, and data might no longer reside on its own technology infrastructure. Instead, all of these resources may reside in a technology center shared with other organizations and managed by a third-party seller [5].

This definition of cloud computing suggests, the cloud can shelter software and data. The cloud form may be used on a project basis for sharing resources between locations.

The cloud may hold entire databases or form information. Because there are many types of cloud based applications, and each applications should be reviewed by the organization before use to define who has access and responsibility for protecting the data and related software in the cloud.

The National Institute of Standards and Technology (NIST) definition of cloud computing identifies four distinct "deployment models" and three kinds of "service models," which are also sometimes also referred to as "delivery models" [1].

Deployment models include the following:

- Private Cloud
- Community Cloud
- Public Cloud
- Hybrid Cloud

Private Cloud infrastructure is "provisioned for exclusive use by single organization comprising multiple consumers (e.g., business units)".

Community Cloud is "provisioned for use by a specific community of consumers from organizations that have shared concerns".

Public Cloud is "provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them".

Hybrid Cloud is "a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities" but also "bound together by standardized or proprietary technology that enables data and application portability".

Cloud computing also provides three important services (or delivery) models:

- Software as a Service (or SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Many authors defend that for cloud computing to be fully realized users will have to be confident that their personal information is protected and their data is both secure and accessible [6, 7, 8].

Users have at least four kinds of worries along these lines. One concern is "how users can control their data stored in the cloud". Currently, users have very little control over or direct knowledge about how their information is transmitted, processed or stored.

Despite these concerns, Cloud offers flexibility and security to users, which do not have to scare about protecting their own data. Cloud enables users to work local with inexpensive platforms.

Jaydip Sen in [9] says, "Cloud computing can only be effective if users and businesses trust cloud service providers".

III. HISTORY AND EVOLUTION

The concept of cloud computing is not new. The power and scale of the cloud has changed highly from what it was in the beginning.

Day by day the technology and business environments had developed, and the status of cloud computing has changed. Cloud computing was the same in principle, but the uses in information today have changed by an enormous degree.

The history of Cloud Computing dates back to the 1960s, when John McCarthy opined that "computation may someday be organized as a public utility" cited in [10].

All the modern-day features of cloud computing were explained in Douglas Parkhill's 1966 book, "The Challenge of the Computer Utility." Some analysts believe that Cloud Computing's find its root back in the year 1950s by Herb Grosch [11].

At the end of the 1990s, some companies such as Sun Microsystems began touting what seemed the marketing concept that "the network is the computer". That idea that Oracle founder Larry Ellison had for terminal machines that would cost less than $300.

These ideas were indeed wise, but they never really took off as consumers were looking for personal computer solutions that had some storage capacity.

The rise of the Internet beginning in the mid-90s changed how computers could be used and how information could be spreaded. With the idea of utility computing long gone, companies such as Amazon began to harness the power of server farms to offer a gaggle of products to would be buyers. Amazon was the first and a most important company built on the foundations of technical innovation beginning especially after the dot-com bubble age. The motivations behind most dot-com companies at that time were not based on profit but on traffic.

Also, in the 1990s, telecommunications companies started offering virtualized private network connections. The newly offered virtualized private network connections had the same service quality as there dedicated services at a reduced cost. Instead of creating physical infrastructure to allow for more users to have their own connections, telecommunications companies were now able to provide users with shared access to the same physical infrastructure.

This list explains the evolution of cloud computing:

- Grid computing: Solving large problems with parallel computing.
- Utility computing: Offering computing resources as a metered service.

- SaaS: Network based subscriptions to applications
- Cloud computing : Anytime, anywhere access to IT resources delivered dynamically as a service [12].

The development of public cloud platforms such as AWS, Microsoft Azure, and Google Cloud Platform, allow external developers to utilize these large-scale services to build new and interesting services and products, benefiting from the economies of scale of large datacenters and the ability to grow and shrink computing resources on demand across millions of customers.

IV. Cloud Computing Stack

Cloud Computing is a broad term for a wide range of services. It is first important to understand what are the different components of Cloud. The Cloud stack comprises of three computing services, generally named as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), which are explained in the next sections.

A. Software as a Service: SaaS

SaaS is defined as a software that is distributed over the Internet. With SaaS, a provider licenses an application to customers either as a service on demand, through a subscription, in a "pay-as-you-go" model, or (increasingly) at no charge when there is opportunity to generate revenue from streams other than the user, such as from advertisement or user list sales [13].

Fig. 1. SaaS (Software as a Service) diagram

SaaS is widely accepted that have been introduced to the business world by the Salesforce company [14]. Other examples are Google Docs, IBM SmartCloud Docs, IBM SmartCloud Meetings, Saleforce.com's CRM application and so on [12].

In some cases SaaS may not be the best option. While it is so valuable tool, there are certain situations that we believe it is not best option for software delivery.

For example, applications where extremely fast processing of real time data is required and legislation or other arrangements do not permit data being hosted externally.

B. Platform as a Service: PaaS

PaaS provides the combination of both, infrastructure and application. Therefore, organizations using PaaS don't have to worry for infrastructure nor for services.

PaaS is similar to SaaS except that, rather than being software delivered over the web, it is a platform for the creation of software, delivered over the web.

Fig. 2. PaaS (Platform as a Service) diagram.

There are a number of different takes on what forms PaaS but some basic characteristics include [15]:

- Services to develop, test, deploy, host and maintain applications in the same integrated development environment. All the varying services needed to answer the application development process.
- Web based user interface creation tools help to create, modify, test and deploy different UI scenarios

PaaS is similar in some ways to Infrastructure as a Service (IaaS). PaaS is especially useful in any situation where multiple developers will be working on a development project or where other external parties need to interact with the development process. For example sales information from a customer relationship management tool, which want to create applications. Finally PaaS is useful where developers wish to automate testing and deployment services.

In some cases, PaaS could not be the best option. For example:

- Where the application needs to be highly portable in terms of where it is hosted.
- Where a special language would hinder later moved to another provider , concerns are raised about vendor lock-in [13].

C. Infrastructure as a Service: IaaS

Infrastructure as a Service (IaaS) is a way of delivering Cloud Computing infrastructure – servers, storage, network and operating systems – as an on demand service. Rather than purchasing servers, software, datacenter space or network equipment, clients instead buy those resources as a fully outsourced service on demand [16].

Some of the most characteristics of IaaS are:

- Resources are distributed as a service
- Allows for dynamic scaling
- Has a variable cost, utility pricing model
- Generally includes multiple users on a single piece of hardware [12].

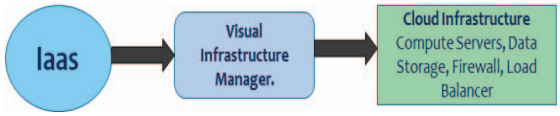

Fig. 3. IaaS (Infrastructure as a Service) diagram.

In some cases , IaaS makes sense. For example:

- Where demand is very volatile – any time there are significant spikes and troughs in terms of demand on the infrastructure.
- Where the organization is growing rapidly and scaling hardware would be problematic [13].

Also in some cases IaaS may not be the best option. For example:

- Where the highest levels of performance are required, and on-premise or dedicated hosted infrastructure has the capacity to meet the organization's needs.

V. Examples of Cloud Computing

In this section we describe the three most popular cloud computing services: Google Drive, Apple iCloud, and Amazon Cloud Drive.

Google Drive: This is a pure cloud computing service, with all the storage found online so it can work with the cloud apps: Google Docs, Google Sheets, and Google Slides. Drive is also available on more than just desktop computers, because we can use it on tablets like the iPad or on smartphones, and there are separate apps for Docs and Sheets, as well. In fact, most of Google's services could be considered cloud computing: Gmail, Google Calendar, Google Maps, and so on (see Figure 4).

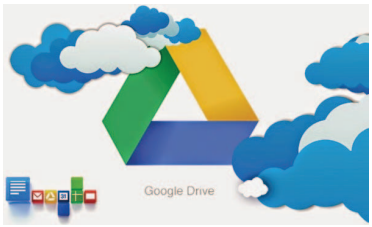

Fig. 4. Google Drive (from http://www.diolinux.com.br/).

Apple iCloud: Apple's cloud service is firstly used for online storage, backup, and synchronization of email, contacts, calendar, and more. All the data we need is available on iOS, Mac OS, or Windows device (Windows users have to install the iCloud control panel). Naturally, Apple won't be outdone by rivals: it offers cloud-based versions of its word processor (Pages), spreadsheet (Numbers), and presentations (Keynote) for use by any iCloud subscriber. iCloud is also the place iPhone users go to utilize the Find My iPhone feature that's all important when the handset goes missing (see Figure 5).

Fig. 5. Apple iCloud (from www.icloud.com/).

Amazon Cloud Drive: Storage at the big retailer is mainly for music, preferably MP3s that is purchased from Amazon, and images - if we have Amazon Prime, we get unlimited image storage. Amazon Cloud Drive also holds anything you buy for the Kindle. It's essentially storage for anything digital you'd buy from Amazon, baked into all its products and services (see Figure 6).

Fig. 6. Amazon Cloud Drive (from www.tekrevue.com).

Hybrid services like Box, Dropbox, and SugarSync all say they work in the cloud because they store a synced version of files online, but they also sync those files with local storage (see Figure 7). Synchronization is a cornerstone of the cloud computing experience, even if we do access the file locally.

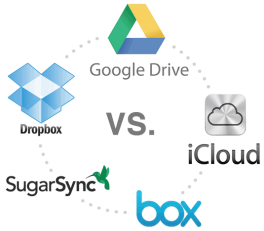

Fig. 7. Hybrid Services (from http://blog.fixya.com/).

VI. Cloud Computing in the Future

Cloud computing is definitely a type of computing paradigm/architecture that will remain for a long time to come. In the near future, cloud computing can emerge in various directions. One possible scenario for the future is that an enterprise may use a distributed hybrid cloud as illustrated in Figure 8.

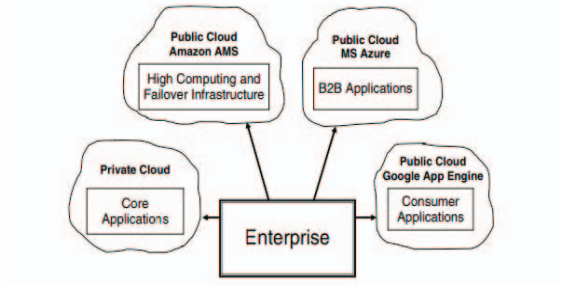

Fig. 8. Distributed hybrid cloud architecture.

In the next sections we give some predictions about cloud computing future.

A. *Cloud Infrastructure Commoditizes and Prices Fall*

Cloud computing already provides a pricing advantage to end users, who gain access to high-end applications at entry-level prices. But the infrastructure, upon which the rest of the cloud lives, will also decrease in price as more major players enter into the market to provide commodity infrastructures to hold the increasing number of cloud applications. Meanwhile,

the competition is steepening. Together, this will make it even cheaper for applications providers to enter into the market.

B. Open Standards Emerge as Dominant in Cloud Platforms

Cloud-based development becomes simpler, giving rise to greater competition from smaller players. It's " dejá vu all over again" as the special shakeout gives way to open systems. These open systems not only simplify development and provide for stronger applications, they allow for a greater level of customization, and they also answer the sad question of what happens to an application if a provider goes out of business.

C. A New Wave of Entrepreneurship Emerges

With cloud computing, users in the next great dotcom boom, will cause a new wave of Entrepreneurship. Cloud computing has lowered the barriers to entry so that anyone can be a dotcom superstar. Entrepreneurs won't need to be programming wizards or enterprise backed. They only need an idea, ambition and a credit card.

D. Smart Phones Evolve With Cloud Apps

Smart phones like the iPhone and Samsung continue to gain functionality and power, and their reach extends further with easier access to wireless broadband. This makes smart phones more attractive as an actual working machine, and a tool for accessing productivity apps over the cloud for corporate use.

E. Social Networking Systems Will Grow Into Collaborative Management Systems

Today's managers need to get things done despite growing challenges. Their teams are more scattered and complex, with more difficulty to motivate, coordinate and hold accountable. An honest manager will tell us that real work is still being done with spreadsheets and emails. For these reasons and more, the future of cooperation will be more focused on the emerging needs of mangers who are coping with more complexity and demands. They need more than social networking. They need interactive management systems with real reports.

VII. Benefits of Cloud Computing

Cloud computing offers many benefits. It allows we to set up what is essentially a virtual office to give the flexibility of connecting to our business anywhere, any time. With the growing number of web-enabled devices used in today's business environment (e.g. smartphones, tablets), access to data is even easier. There are many benefits to move the business to the cloud, but also some problems as we see in the next sections.

A. Advantages

Cloud computing offers many benefits and advantages both to users and businesses of all sizes.

a. Save Money

One of the most significant cloud computing benefit is cost saving. Application of cloud computing reduces the costs of electronic data management.

b. Save Time

There is no installation, and the SaaS provider takes care of updates, including security, and is responsible for data storage and retrieval.

c. Staying Current

Provide immediate access to the latest innovations and updates at the provider's costs.

d. Service

We can get better service from a supplier. If we are thinking SaaS, we can ask a supplier about a service level agreement. A good agreement should guarantee both a certain level of uptime for the product and an answer time for technical and support service requests.

B. Disadvantages

Cloud computing has certainly benefited many enterprises by reducing costs and allowing them to concentrate on their core business authority and infrastructure issues. But there are still clear disadvantages of Cloud Computing, such as downtime, security, and limited control.

a. Downtime

Number of clients are taken care each day in cloud service providers. They can become crushed and may even come up against technical interruption. This can cause the business processes being temporarily suspended.

Additionally, if Internet connection is offline, you will not be able to access any of your applications, server or data from the cloud.

b. Security

Cloud service providers implement the best security standards and industry certifications, but storing data and important files on external service providers always opens to risks.

When using cloud computing it is necessary to supply the service provider with access to important business data. At the same time, to be a public service opens up cloud service providers to security challenges on a routine basis.

The facility in supplying and accessing cloud services can also give unscrupulous users the ability to scan, identify and exploit escapade and vulnerabilities within a system.

For example, in a multi-tier cloud architecture where several users are hosted on the same server, a hacker might try to break into the data of other users hosted and stored on the same server. However, such events and exploits are probably not for everyone, and the probability of occurrence of is not great.

c. Limited Control

Since the cloud infrastructure is completely owned, managed and monitored by the service provider, it transfers minimal control over to the customer.

The customer can only control and manage the applications, data and services operated on top of that, not the back end infrastructure itself. Key administrative tasks such as server shell access, updating and firmware management may not be passed to the customer or end user.

VIII. HACKER ETHIC

"Hacker" is defined such as someone enthusiastic and ambitious about computer work (or, for that matter, any kind of work activity: it is that attitude that counts). In the popular mind, hacker means someone who "hacks" their way into cyberspace where they don't belong (Pentagon, bank records, etc.).

A new "ethic" is described that is completing the older "Protestant work ethic" described famously by sociologist Max Weber.

First, rather than a terrible Calvinistic duty, work in the hacker ethic is full of passion, joy, and entertainment.

Second, rather than being motivated by monetary gain, the hacker attitude toward money is cavalier: hackers share widely and freely what they have (as Linus Torvalds has with the Linux operating system).

Thirdly, hacker social relations occur in a web-facilitated network of free and open exchange of ideas and of ready access to all the people [17].

The hacker ethic is described as [18]:

- Accesing to computers should be unlimited and total
- All informations should be free
- Hackers should be judged by their hacking.
- You can create art and beauty on a computer
- Computers can change your life for the better.

Some of the early hackers believed that computer systems were naturally flawed and thus needed to be improved.

As a result, some hackers believed that they needed total access to all computer systems in order to take them apart, see how they work, and make the needed improvements. In real these hackers wanted to remove any barriers to free access to computers.

Many hackers have embraced and some continue to embrace, either directly or indirectly, the following three principles [18]:

- Information should be free.
- Hackers provide society with a useful and important service.
- Activities in cyberspace are virtual in nature and thus do not harm real people in the real (physical) world.

A. Examples of Ethical Hacking

It is humorous, as a result of the idea of finishing up what's basically a malicious assault ethically has definitely developed people's understanding on the subject of hacking. People tend to immediately affiliate this with harmful actions and intentions, as a result of they just know the harmful effects. In short, most will believe there might be little or no constructive benefit for it, but of course that is just not true. If it is used for good things, it's good.

When used as a means to improve a person or an organization's online defenses, we find this "malicious act" more or less beneficial. The apply of breaking into, or bypassing an internet system or community in an effort to expose its mistake for additional increase is fully ethical.

Examples of ethical hacking include exploiting or exposing a website so as to discover its weak points. Then report findings and let the suitable particular person fix these vulnerabilities. Then in the future, ought to they arrive beneath assault, they will be that bit safer. If we are actually preparing them for any actual threat of assault since we are eliminating the areas which could possibly be exploited against them.

There are a lot of examples of ethical hacking, together with one which happened within the early days of computers. The United States Air Force used it to conduct a security analysis of an operating system. In doing so, they had been in a position to discover mistakes like vulnerable hardware, software program, and procedural security. They decided that even with a relatively low degree of effort, their security might be bypassed and the uninvited guest would get away with precious information.

Thanks to moral hacking, they have been in a position to cease such an incident from happening. The people who carried out this job treated the situation as if they really were the enemy, doing all they may to interrupt into the system. This way, they could decide exactly how secure their system was. That is maybe top-of-the-line examples of moral hacking as a result of they were confirmed by the people who were responsible for the creation of the stated online system. They confirmed the need for such motion as a result of they know that there are lots of people able to doing the same factor, or inflicting the same hurt to their system.

From all the examples of moral hacking, maybe you possibly can clearly relate to the practices of identified Working Systems being used today. Makers of those Working Programs perform their own moral hacks to their systems earlier than actually launching their products to the public. This is to prevent potential assaults that may very well be handled by hackers.

This is by some means a method of quality control during the system's improvement phase, to be sure that all of the weaknesses of their Working Methods are covered, since will probably be marketed for public use. Ethical hacking is a really useful method in defending your treasured online systems. By clapping into the talents and potential of white hat hackers, you are able to take on and prevent damages caused by the actual hackers.

IX. CYBER SECURITY

Cyber security is referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.

Cyber security is important because governments, military, corporations, financial institutions, hospitals and other businesses collect, process and store a great deal of secret information on computers and transmit that data across networks to other computers.

With the growing volume and sophistication of cyber attacks, continuing attention is required to protect sensitive business and personal information, as well as protect national security [19].

Ethics are an important part of cyber security. In countless organizations IT personnel are trusted with the ability to access sensitive and personal data.

We learn our ethics from early age, what is true and what is wrong. As we grow up, we are influenced by the actions of those around us. Hopefully we are surrounded by ethical people to act as role models for us in our lives. Ethics come from oldness where it was felt that one should look to the common good in making decisions and at the least do no harm when making those decisions.

In Washington, DC., the Computer Ethics Institute has developed a list of ethical behaviors to live by that may become a starting point for discussion when asking ethical questions. Several of these behaviors may be useful to start a conversation at home or workplace about computer ethics in our society. These behaviors are [20]:

- When using a computer, don't harm others…..be respectful of all.
- Stay out of and don't steal other people's work, files, software, etc.
- Don't use other people's work without citing or paying for it.
- Think first of the social consequences of what you are doing.

A. Risk Analysis in Cyber Security

It has a wide range of sectors, including commerce. For example, banks and credit card companies can tolerate an important amount of credit risk because they know how to guess losses and how to price their services accordingly.

In securing computer systems, the level of risk can be different. For example, can a mere cost-benefits analysis be applied to computer security issues that impact the safety and lives of individuals? Financial considerations alone might be enough for determining the "bottom line" for some corporations and organizations deciding how to increase their computer security.

Risk can be understood and analyzed in terms of the net result of the impacts of five elements. These are [18]:

- Assets
- Threats
- Vulnerabilities
- Impact
- Safeguards.

B. Cyber Security and the Cloud

Using the Cloud brings a lot of benefits, but it also brings risk. Research shows that 51% of organizations are unwilling to migrate to the Cloud due to concerns about data security flaws.

When considering moving data to the Cloud, organizations often find it difficult to compare and evaluate the effectiveness of various Cloud providers' data security practices. As a result, Cloud providers are increasingly being asked to show that they have the necessary controls in place to manage Cloud-related risks. A growing number of requests demand evidence of compliance with leading security standards.

IT Governance offers a range of products and services that will help Cloud providers to implement the necessary controls for achieving the required level of security that their customers demand.

X. CONCLUSIONS

This paper summarized what is cloud computing and what is ethic in cloud computing. Cloud Computing evolved by consolidating several technologies like SaaS, PaaS, IaaS. Also, this work suggested some solutions and the issues were enriched with given examples. Cloud computing presents a cost-effective storage solution, but also creates risks to the security of secret client information. With right diligence process and conceivable care, users can avoid the ethical dangers of cloud computing.

We think Cloud Computing is the fastest growing part of network based computing. It provides enormous benefits to customers of all sizes: simple users, developers, enterprises and all types of organizations. We hope that this paper helps practitioners who are interested in ethics in cloud computing.

REFERENCES

[1] P. Mell and T. Grance, "NIST Definition of Cloud Computing", National Inst. Standards and Technology, September, 2011, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[2] Computer Weekly, "Deperimeterization changing today's security practices", June 2009, http://www.computerweekly.com/feature/Deperimeterization-changing-todays-security-practices

[3] Dan C. Marinescu. Cloud Computing Theory and Practice. Elsevier Inc., 2013, Pages 14 . http://eclass.uoa.gr/modules/document/file.php/D416/CloudComputingTheoryAndPractice.pdf

[4] Committee of Sponsoring Organizations of the Treadway Commission (COSO). http://www.coso.org/

[5] Journal of Integrative Humanism vol. 6 No 1, 1. Edition page 161. Faculty of Arts University of Cape Coast, Ghana, February 15, 2016

[6] Ann Cavoukian, "Patience, Persistence, and Faith: Evolving the Gold Standard in Privacy and Data Protection". 26th IFIP TC 11 International Information Security Conference, SEC 2011, Lucerne, Switzerland, IFIP Advances in Information and Communication Technology 354, Springer 2011, pp. 1-16.

[7] Ann Cavoukian, Alan Davidson, Ed Felton, Marit Hansen, Susan Landau, Anna Slomovic, "Privacy: Front and Center". IEEE Security & Privacy 10(5): 10-15 (2012).

[8] Michelle Chibba, Ann Cavoukian, "Privacy, consumer trust and big data: Privacy by design and the 3 C'S". ITU Kaleidoscope: Trust in the Information Society, Barcelona, Spain 2015, pp. 1-5

[9] Sen, J. Security and Privacy Issues in Cloud Computing. In Martinez, A. R., Marin-Lopez, R., and Pereniguez-Garcia, F., editors, Architectures and Protocols for Secure Information Technology Infrastructures, pp 1–45. IGI Global 2013. https://arxiv.org/pdf/1303.4814.pdf

[10] Inderveer Chana and Tarandeep Kaur, "Delivering IT as A Utility- A Systematic Review". International Journal in Foundations of Computer Science & Technology (IJFCST), Vol. 3, No.3, May 2013 Thapar University, India https://arxiv.org/ftp/arxiv/papers/1306/1306.1639.pdf

[11] Herb Grosch, Columbia University Computing History. http://www.columbia.edu/cu/computinghistory/grosch.html

[12] IBM Thoughts On Cloud bloggers team. Cloud Computing Simplified: The Thoughts on Cloud Way. IBM RedBlook: http://www.redbooks.ibm.com/redpapers/pdfs/redp5179.pdf

[13] Ben Kepes, "Understanding the cloud computing stack SaaS, PaaS, IaaS", http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Understanding-the-Cloud-Computing-Stack.pdf

[14] Salesforce company. http://www.salesforce.com/.

[15] Chris Keene, "What Is Platform as a Service (PaaS)?", https://dzone.com/articles/what-platform-service-paas, March 2009

[16] Ben Kepes, "Moving your Infrastructure to the Cloud - How to Maximize Benefits and Avoid Pitfalls". http://diversity.net.nz/wp-content/uploads/2011/01/Moving-to-the-Clouds.pdf

[17] David W. Gill, Building Ethically Healthy Organizations, www.ethixbiz.com

[18] Herman T. Tavani. Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing, 5th Edition, Wiley, December 2015.

[19] Cyber Security Primer, University of Maryland : http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm

[20] Alfred Thomson, Ten Commandments of Computer Ethics, https://blogs.msdn.microsoft.com/alfredth/2012/08/29/ten-commandments-of-computer-ethics/, 2014